SHUSAKU YAMAMOTO

Japanese Patent No. 2884338

(Translation)

Japanese Patent No. 2884338

Issuance date: April 19, 1999
Registration date: February 12, 1999
Application number: 9-264850
Divisional application: divisional application based on:
Japanese Application No. 8-56966
Filing date: October 11, 1984
Request for examination filed on: October 13, 1997

The patentee is prepared to assign or license the patent right.

Application for expedited examination

Patentee: Yutaka TSUKAMOTO

Inventor: Yutaka TSUKAMOTO

[Title of the Invention] Access control system

[Claims]

1. An access control system for performing authentication based on password data generated by an access demanding side and thus performing access control, the access control system comprising:

a plurality of access targets to which the access demanding side attempts to access, the plurality of access targets being located at a plurality of positions in a discrete manner;

authentication means for performing centralized management by performing comprehensive authentication for access control when an access is requested to each of the plurality of access targets; and

variable password data generation means, having a calculation processing function, for generating password data at the access demanding side, wherein variable password data is generated, a content of which is variable on an access-by-access basis, by a calculation utilizing commonly changing data which commonly changes both in the access demanding side and the authentication means side,

wherein:

when the access demanding side transfers the variable password data in order to access any of the plurality of access targets, the variable password data is forwarded to the authentication means,

the variable password data generation means has a clock function and generates the variable password data by utilizing, as the commonly changing data, time variable data which varies in accordance with time counted by the clock function, and

the authentication means includes time synchronous authentication means for performing authentication by determining whether the forwarded variable password data is appropriate or not by using, as the commonly changing data, the time variable data which changes in accordance with time,

the access control system further comprising:

automatic error correction means for, when an error occurs in the time variable data by a malfunction of the clock of the variable password data generation means, automatically correcting the error so that over-time accumulation of the errors can be prevented,

wherein the access demanding side is permitted to access the access targets on the conditions that an authentication result indicating it is appropriate is obtained by the authentication means.

2. An access control system for performing authentication based on password data generated by an access demanding side

and thus performing access control, the access control system comprising:

a plurality of access targets to which the access demanding side attempts to access, the plurality of access targets being located at a plurality of positions in a discrete manner;

authentication means for performing centralized management by performing comprehensive authentication for access control when an access is requested to each of the plurality of access targets; and

variable password data generation means, having a calculation processing function, for generating variable password data at the access demanding side, wherein variable password data is generated, a content of which is variable on an access-by-access basis, by a calculation utilizing commonly changing data which commonly changes access by access both in the access demanding side and the authentication means side,

wherein:

when the access demanding side transfers the variable password data in order to access any of the plurality of access targets, the variable password data is forwarded to the authentication means,

the variable password data generation means has a clock function and generates the variable password data by utilizing, as the commonly changing data, time variable data which varies in accordance with time counted by the clock function, and

the authentication means includes time synchronous authentication means for performing authentication by determining whether the forwarded variable password data is appropriate or not by using, as the commonly changing data, the time variable data which changes in accordance with time,

the time synchronous authentication means further comprising:

prescribed tolerable error authentication means which, even when the forwarded variable password data is generated by the time variable data having an error, does not prohibit an access based on the error when the error is within a prescribed tolerable time period; and

unauthorized access prohibition means for prohibiting the access when an access is made by variable password data which is identical with the variable password data used for a preceding access within the tolerable time period from the preceding access.

3. An access control system according to claim 1 or 2, wherein the variable password data generation means includes identification signal input determination means for determining that an identification data signal for confirming a person possessing the variable password data generation means is input, and the variable password data is allowed to be generated on the conditions that the input determination is performed by the identification signal input determination means.

4. An access control system according to claim 1 or 2, wherein the authentication means executes a password authentication operation on the conditions that the password is confirmed to be appropriate based on registration confirmation data, notified by the access demanding side, for confirming whether the access demanding side is registered beforehand or not, the confirmation of the password being performed before the authentication means performs the password authentication operation based on the variable password data.

[Detailed Description of the Invention]

[0001]

[Field of the Invention] The present invention is mainly an access control system for authenticating whether or not an access to access target equipment should be permitted in or-

der to restrict the access target equipment to be accessed only by a specific person and thus performing access control, and particularly relates to an access control system, by which an access demanding side transfers password data by data communication and the access control is performed based on the transferred password data.

[0002]
[Prior Art] Conventionally and commonly known access control systems of this type include, for example, a system described in Japanese Laid-Open Publication No. 59-10680. This conventional system is structured to operate as follows. A prescribed secret rule (data for determining whether or not the password data is appropriate) is registered in access target equipment beforehand. Random numbers generated on the side of the access target equipment are input to a password data generation apparatus possessed by the access demander, and password data generated using the random numbers is transferred to the access target equipment side. Only when the password data generated using the secret rule registered on the access target equipment side matches the transferred password, the access demander is determined to be appropriate and permitted to access the access target equipment. In other words, commonly changing data which can change on an access-by-access basis and can commonly change on the access demanding side and the access target equipment side is structured of the random numbers. Using the commonly changing data, the password data which can change each time to authenticate whether or not the access should be permitted.

[0003] However, in the case where these types of access control systems spread in the highly information-oriented society, the systems are more frequently used for, for example, unlocking coin locker doors, calling the people's own bank accounts, and calling secret technological information hav-

ing limited users from file apparatuses or the like. Thus, the systems are used for accessing many pieces of access target equipment. As a result, the data for determination such as the secret rule or the like needs to be registered in each and every piece of access target equipment which the user demands to access. Thus, opportunities for the others to misappropriate the registered data for determination is increased. This generates a defect that serious damage is caused by such abuse. Especially in the highly information-oriented society, there should never be any leak of individual privacy or company secrets. The above-mentioned misappropriation of the data for determination must be strictly prevented.

[0004]

[Problems to be Solved by the Invention] It is conceivable that different data for determination for each of the pieces of access target equipment are registered, so that even if one of the data for determination is stolen, the stolen data cannot be used to access the other pieces of access target equipment. However, this is troublesome since the user needs to memorize or possess the data for determination used for each piece of access target equipment. Especially when the number of pieces of access target equipment is large, the user can possibly forget the data. Thus, this method is inconvenient.

[0005] Even if the misappropriation of the registered data for determination can completely be prevented, the above-mentioned method has the following defects in the case of the conventional system by which the above-described data for determination is registered in all the many pieces of access target equipment. The troublesome work of registering the data for determination in all the many pieces of access target equipment is required. Moreover, when the data for determination needs to be updated for the reason that

the password data generation apparatus is stolen or the like, all the data for determination registered in all the many pieces of access target equipment needs to be updated. This requires very troublesome work. The present invention conceived in light of these circumstances has an objective of providing an access control system for, even when the number of pieces of access target equipment is increased, eliminating the necessity of registering the data for determination in all the many pieces of access target equipment so as to prevent various inconveniences described above caused by registering the data for determination for each piece of access target equipment.

[0006]

[Means for Solving the Problems] The first invention is an access control system for performing authentication based on password data generated by an access demanding side and thus performing access control, the access control system comprising a plurality of access targets to which the access demanding side attempts to access, the plurality of access targets being located at a plurality of positions in a discrete manner; authentication means for performing centralized management by performing comprehensive authentication for access control when an access is requested to each of the plurality of access targets; and variable password data generation means, having a calculation processing function, for generating password data at the access demanding side, wherein variable password data is generated, a content of which is variable on an access-by-access basis, by a calculation utilizing commonly changing data which commonly changes both in the access demanding side and the authentication means side, wherein when the access demanding side transfers the variable password data in order to access any of the plurality of access targets, the variable password data is forwarded to the authentication means; the variable password data generation means has a clock function and gen-

erates the variable password data by utilizing, as the commonly changing data, time variable data which varies in accordance with time counted by the clock function; and the authentication means includes time synchronous authentication means for performing authentication by determining whether the forwarded variable password data is appropriate or not by using, as the commonly changing data, the time variable data which changes in accordance with time. The access control system further includes automatic error correction means for, when an error occurs in the time variable data by a malfunction of the clock of the variable password data generation means, automatically correcting the error so that over-time accumulation of the errors can be prevented, wherein the access demanding side is permitted to access the access targets on the conditions that an authentication result indicating it is appropriate is obtained by the authentication means. The second invention is an access control system for performing authentication based on password data generated by an access demanding side and thus performing access control, the access control system comprising a plurality of access targets to which the access demanding side attempts to access, the plurality of access targets being located at a plurality of positions in a discrete manner; authentication means for performing centralized management by performing comprehensive authentication for access control when an access is requested to each of the plurality of access targets; and variable password data generation means, having a calculation processing function, for generating password data at the access demanding side, wherein variable password data is generated, a content of which is variable on an access-by-access basis, by a calculation utilizing commonly changing data which commonly changes access by access both in the access demanding side and the authentication means side, wherein when the access demanding side transfers the variable password data in order to access any of the plurality of access targets, the variable password

data is forwarded to the authentication means; the variable password data generation means has a clock function and generates the variable password data by utilizing, as the commonly changing data, time variable data which varies in accordance with time counted by the clock function; and the authentication means includes time synchronous authentication means for performing authentication by determining whether the forwarded variable password data is appropriate or not by using, as the commonly changing data, the time variable data which changes in accordance with time. The time synchronous authentication means further includes prescribed tolerable error authentication means, even when the transmitted variable password data is generated by the time variable data having an error, which does not prohibit an access based on the error when the error is within a prescribed tolerable time period; and unauthorized access prohibition means for prohibiting the access when an access is made by variable password data which is identical with the variable password data used for a preceding access within the tolerable time period from the preceding access.

[0007]

[Function] According to the first invention, authentication means for performing authentication comprehensively to a plurality of access targets discretely located is provided. When an access request is made to each of the plurality of access targets, the authentication means performs centralized management by performing comprehensive authentication for access control. By the action of the variable password data generation means, having a calculation processing function, for generating variable password data at the access demanding side, variable password data is generated, a content of which is variable on an access-by-access basis, by a calculation utilizing commonly changing data which commonly changes both in the access demanding side and the authentication means side. When the access demander forwards the

variable password data in an attempt to access either one of the plurality of access targets, the variable password data is forwarded to the authentication means. The variable password data generation means has a clock function, and generates the variable password data using, as the commonly changing data, time variable data which varies in accordance with time counted by the clock function. The authentication means includes time synchronous authentication means for performing authentication by determining whether the forwarded variable password data is appropriate or not by using, as the commonly changing data, the time variable data which changes in accordance with time. By the action of the automatic error correction means, when an error occurs in the time variable data by a malfunction of the clock of the variable password data generation means, the error is automatically corrected so that the over-time accumulation of the errors can be prevented. The access demander is permitted to access the access target on the conditions that an authentication result indicating it is appropriate is obtained by the authentication means. According to the second invention, authentication means for performing authentication comprehensively to a plurality of access targets discretely located is provided. When an access request is made to each of the plurality of access targets, the authentication means performs centralized management by performing comprehensive authentication for access control. By the action of the variable password data generation means, having a calculation processing function, for generating variable password data at the access demanding side, variable password data is generated, a content of which is variable on an access-by-access basis, by a calculation utilizing commonly changing data which commonly changes both in the access demanding side and the authentication means side. When the access demander forwards the variable password data in an attempt to access either one of the plurality of access targets, the variable password data is forwarded to the authen-

tication means. The variable password data generation means has a clock function, and generates the variable password data using, as the commonly changing data, time variable data which varies in accordance with time counted by the clock function. The authentication means includes time synchronous authentication means for performing authentication by determining whether the forwarded variable password data is appropriate or not by using, as the commonly changing data, the time variable data which changes in accordance with time. By the action of the prescribed tolerable error authentication means, even if the forwarded variable password data is generated by the time variable data having an error, an access is not prohibited based on the error when the error is within a prescribed tolerable time period. By the action of the unauthorized access prohibition means, when an access is made by variable password data which is identical with the variable password data used for the preceding access within the tolerable time period from the preceding access, such an access is not determined to be permissible.

[0008]

[Embodiments of the Invention] Before describing the embodiments of an access control system according to the present invention, embodiments of a digital signature system which will be increasingly required in data communication in a highly information-oriented society will be described.

[0009] As shown in Figure 1, a personal terminal device 3 including a built-in RAM or CPU is structured to be detachable to a data input apparatus 2 as an example of data input means having a keyboard 1 by which "hiragana" (translation note: Japanese phonetic letters) and numerals can be input by character keys and numeral keys. This personal terminal device can be any device which is individually possessed by a person sending data with an intention of performing digi-

tal signature. Conventionally and commonly known such devices include, for example, an IC card.

[0010] Figure 10 shows a circuit configuration of the personal terminal device 3 possessed by an individual. The personal terminal device 3 accommodates a CPU 50, a ROM 51, a RAM 52, and an I/O port 53. The ROM 51 stores therein an operation program of the CPU 50, i.e., a program shown in a flowchart of Figure 2 described below or the like. The CPU 50 operates in accordance with the program stored in the ROM 51, and calls a character-numeral conversion rule or a secret function as an example of a secret rule described below and causes the rule to be stored in the RAM 52. As described below, sending data which has been input from the keyboard 1 through the I/O port 53 is converted as shown in Figure 2 by an algorithm in accordance with the secret rule stored in the RAM 52. The converted data is output through the I/O port 53.

[0011] The secret rule stored in the personal terminal device 3 is constituted of, for example, a character-numeral conversion rule for converting hiragana letters into numerals in accordance with a certain rule, a secret function f(x) consisting of a combination of trigonometric functions and an exponential function and the like. Different types of secret rules are stored in different personal terminal devices 3. Accordingly, each of the signers attempting to sign possesses the respective personal terminal device 3 to hold his/her own secret rule. The secret rule is secret from others.

[0012] The personal terminal device 3 has the program shown in the flowchart of Figure 2 incorporated therein. For performing digital signature, sending data such as characters of an agreement to be signed or the like is input from the keyboard 1 in the form of hiragana letters while the per-

sonal terminal device 3 is attached to the input device 2. The numerals such as dates or the like are input as they are. When characters are input, each of the characters is converted into a numeral in accordance with the character-numeral conversion rule each time the character is input and the converted numerals are added together. When numerals are input, those numerals are added together. When key E for END is pressed, a sum P(n) of all the characters and numerals is substituted into the secret function f(x) and an answer is found. The converted data, which is the answer consisting of an encrypted code (numeral in this case), is output through the I/O port 53 as signature data and displayed on the display section 4. The signature data displayed on a display section 4 is sent together with the sending data such as the agreement or the like, which is the target of authentication.

[0013] The input device 2 can be a teletex terminal. In this case, the sending data to be signed is input from the keyboard of the teletex terminal to the personal terminal device 3. It is structured that the data for authentication, which is converted data output from the personal terminal device 3, is transferred to the other party of the agreement from the teletex terminal.

[0014] The secret rule consisting of the character-numeral conversion rule and the secret function is registered in, for example, a public institution such as government offices, a service organization or the like having a duty to protect privileged information.

[0015] In the case of digital signature for performing authentication for checking, such as a document acceptance stamp, a receipt stamp, money receipt stamp or the like, the act to be authenticated such as document acceptance or the like is input in hiragana letters from the keyboard 1, and

the date of the act to be authenticated is input. Thus, the converted data, i.e., signature data, is calculated. When, for example, the act to be authenticated is document acceptance and the date of authentication is October 9, 1984, 11:35 (eleven thirty-five), "しょるいうけつけ1984ねん10がつ9ひ11じ35ふん" is input from the keyboard 1. (Translation note: hiragana letters are included in the above phrase as discussed above.)

[0016] It can be structured that one-touch input is possible by allocating various representative checking acts such as document acceptance, receipt and the like to one operation key of the keyboard 1.

[0017] Needless to say, the acts of document acceptance, receipt and the like listed as the acts to be authenticated in the sense of the present invention are mere examples, and the acts to be authenticated includes various checking acts such as an act of ordering, an act of delivering a product, an act of receiving money, and the like in the case of authentication of order sheets, statements of delivery, receipts and the like.

[0018] Next, other examples will be described.

(1) Instead of using a numeral obtained by a secret function as signature data as it is, a part or the entirety of the obtained numeral is converted into characters such as hiragana letters, "katakana" (translation note: Japanese phonetic letters), Chinese characters, alphabetical letters or the like, or graphics or symbols, or combinations thereof, or combinations thereof with colors, based on a certain secret rule, to be used as signature data.

[0019] (2)The secret rule is stored in a file apparatus 5 of a corporation or the like as shown in Figure 3, instead

of being stored in the personal terminal device 3. In such a case, the teletex terminal 6 and the file apparatus 5 are connected to each other through a LAN 8 or the like via a computer 7. A signer of a paperless transaction performed with another corporation utilizing public telephone lines or the like calls his/her own secret rule by operating the teletex terminal 6 and performs encryption or other conversion works by the computer 7. When the secret rule is called, an individual identification system described below is utilized to check by the computer 7 whether or not the secret rule specified by the signer really belongs to the signer. Only when the secret rule is confirmed to belong to the signer, an access of the signer to the specified secret rule is realized.

[0020] In the figure, reference numeral 9 represents a node.

(3) The signer calls his/her secret rule, from a file apparatus of a public institution, service organization or the like in which the secret rule has been registered, or from a file apparatus of his/her house through data communication, instead of from the file apparatus 5 in the corporation; and performs encryption or other conversion works by a computer connected to the called file apparatus.

[0021] (4) The personal terminal device 3 is structured so that the encryption or other conversion function is stopped when a prescribed signal (different by transmitter to transmitter) from a signal transmitter (e.g., of a ring-shape) owned by the owner of the device cannot be received. Thus, abuse by others is prevented when the personal terminal device 3 is lost.

[0022] (5) As a conversion method such as encryption or the like, $P(N)=P(N-1)+N\cdot D(N)$, $P(N)=P(N-1)+D(N)/N$, $P(N)=P(N-$

1)/N+D(N) or P(N)=P(N-1)/N+N·D(N) or the like is used instead of P(N)=P(N-1)+D(N) shown in Figure 2.

[0023] Next, an embodiment of an access control system according to the present invention (individual identification system) will be described. This access control system can also be utilized in order to, for example, when a secret rule is to be read, determine whether or not the specified secret rule actually belongs to the individual who specified the secret.

[0024] As shown in Figure 4, a piece of equipment which should be permitted to be accessed to a certain limited range of people, such as equipment for calling a person's own account in a bank 10, retrieving secret technological information in a data bank 11, unlocking a coin locker 12 or the like is connected via a public telephone line 15 to a computer 13 or 14 in his/her house or in a prescribed institution for performing individual identification on whether or not an equipment user (access demander) may be permitted to access the equipment. It is structured so that data communication is possible between the equipment 10, 11, 12 and the computer 13, 14 for performing the individual identification. In the figure, reference numeral 16 represents a network control unit (NCU), and reference numeral 17 represents a switchboard.

[0025] When, for example, the technological information in the data bank 11 is demanded to be utilized, the data bank 11 is first called by a CAPTAIN terminal 18 so as to retrieve the desired technological information. When the technological information is secret technological information permitted to be used only by certain people, individual identification is performed using the following procedure.

[0026] (1)The equipment user who tries to use the technological information informs the data bank 11 of the calling number of the computer 13 or 14 in his/her house or in a prescribed institution for performing individual identification.

[0027] (2)The data bank 11 checks whether or not the number is registered beforehand and belongs to an individual who can be permitted to obtain a permission of use. If the number belongs to an individual who can be permitted to obtain a permission of use, the data bank 11 requests for transmission of the identification number. If the number does not belongs to an individual who can be permitted to obtain a permission of use, the data bank 11 does not permit the use.

[0028] (3)When the request for transmission of the identification number is issued, the equipment user transmits an identification signal output by his/her device 33 to the data bank 11 by the CAPTAIN terminal 18.

[0029] (4)The data bank 11 transmits the received identification signal to the computer 13 or 14 having the calling number. The computer 13 or 14 performs individual identification determination (described below) on whether or not the received identification number is correct and transmits the result to the data bank 11.

[0030] (5)The data bank 11 permits an access to the specified secret technological information only when a determination result that the identification number is correct is transmitted.

[0031] Next, a procedure for unlocking the coin locker 12 is as follows. First, the calling number of the computer 13 or 14 in the equipment user's house or in a prescribed institution for performing individual identification is input by

operating a keyboard on an internal surface of the door of the coin locker in an unlocked state. The door is closed and locked in the state where the computer 13 or 14 is registered beforehand and the door is set so that the computer 13 or 14 is automatically called when an unlocking operation is performed. For unlocking, the identification signal is input on an external surface of the door, and the unlocking control is performed in a similar method to that in (4) and (5) described above.

[0032] Next, a procedure for calling the user's bank account for, for example, paying money, is as follows in a cashless payment system (bank POS system) or the like, according to which only a numerical figure is transferred, i.e., money in the user's bank account is transferred to the bank account of the money recipient, without transfer of cash. First, the calling number of the computer 13 or 14 in the user's house or in a prescribed institution is registered in the bank beforehand. It is set so that the computer 13 or 14 is automatically called when the user's bank account is specifically called. For making a payment for the purchase done in a supermarket or the like, the user specifically calls his/her bank account from a register 19 of the supermarket or the like, and accesses his/her bank account in a similar manner to that in (4) and (5) described above. As the means for specifically calling his/her bank account, the method of inputting a bank account calling and specifying signal which is output from the device 33 of the equipment user from a register 19 and transferring the signal to the bank is used.

[0033] For an access for unlocking the door of an automobile or the like, or for starting an engine, data communication by a cabled medium such as a public telephone line or the like is unusable since the equipment to be utilized is a movable object. Accordingly, a wireless medium such as sat-

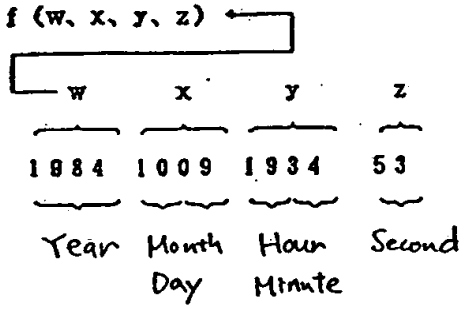
ellite communication or the like is used. Thus, the "data communication" in the sense of the present invention is a broad concept including wireless media as well as cabled media.

[0034] Next, the above-mentioned individual identification method will be described. As shown in Figure 5, the device 33 owned by the equipment user is constituted of a wrist watch for receiving code/data broadcasting such as a time standard radio wave by JJY or the like and displaying the time based on the received signal. The current time displayed by the wrist watch 33 is substituted, as an input signal, into a secret function (different wrist watch by wrist watch) as a secret rule which is stored in the wrist watch 33, and the answer is calculated. The answer and a part of the used input signal corresponding to the second are output as an identification signal. The output is performed as follows. First, as shown in Figure 6, a transmission button 21 is pushed, and the identification signal is sent out for a certain period of time (10 seconds) to a hand 23 from a signal transmission section 22 consisting of a conductive plate on a rear surface of the wrist watch. The identification signal is transmitted to an identification signal receiving section 24 of the register 19, the coin locker 12, the automobile 20, the CAPTAIN terminal 18, a telephone, a teletex terminal or the like, using the hand 23, which is a conductive body, as a medium. The transmitted identification signal is transmitted to the computer 13 or 14 in the user's house or a prescribed institution for performing individual identification determination. The input signal is substituted into a secret function as a secret rule which is registered in the computer beforehand, and the answer is calculated. The answer and the identification signal are compared with each other to determine whether or not the identification signal is correct. Thus, the individual identification determination is performed.

[0035] The secret function is a function consisting of a combination of trigonometric functions, exponential functions and the like, and has four variables w, x, y and z. As in expression 1 shown below, each part of the input signal is substituted into w, x, y and z to calculate the answer.

[0036]

[Expression 1]



[0037] For sending an identification signal from a foreign country to Japan, an input signal obtained by converting the time in that foreign country into Japan time needs to be substituted into the secret function.

[0038] In the figure, reference numeral 25 represents a ring-shape signal transmitter owned by an equipment user for generating a certain signal. The signal is different transmitter by transmitter. The signal transmitter is structured so as to transmit an identification signal only when the wrist watch 33 is receiving a prescribed signal from the transmitter 25. Thus, abuse by others is prevented when the wrist watch 33 is lost.

[0039] In the figure, reference numeral 26 represents a keyboard used for calling the user's bank account or the like. A PIN is input to or a bank account calling and specifying

signal is output from the keyboard. These signals are output from the signal transmission section 22 similarly to the identification signal.

[0040] The wrist watch 33 is structured so as to correct an error from the displayed time incessantly based on the signal by the code/data broadcasting. A flowchart of the program incorporated into the wrist watch 33 is shown in Figure 7. Thus, the wrist watch 33 includes a microcomputer operating in accordance with a program, i.e., a microcomputer having a similar circuit configuration as that shown in Figure 10 built therein.

[0041] The flowchart shown in Figure 7 will be briefly described. By step S (hereinafter, referred as simply to "S") 1, it is determined whether or not a time standard radio wave by the code/data broadcasting has been received. The program waits until the wave is received. When the wave is received, the program advances to S2, where an operation of correcting a frequency divider based on the time standard radio wave and displaying the corrected time is performed. Then, the program advances to S3, where it is determined whether or not a signal from a receiver 25 (see Figure 5) has been received. When the signal has not been received, the program returns to S1. When the signal has been received, the program advances to S4, where it is determined whether or not a receiving button 21 (see Figure 6) of an individual identification signal has been turned ON. When the button has not been turned ON, the program returns to S1. When the button has been turned ON, the program advances to S5, where the process of inputting an input signal consisting of current time to each of w, x, y and z of the secret function f(w, x, y, z) and calculating the answer A is performed. Then, the program advances to S6, where the process of outputting the calculated answer A and a numerical value NZ substituted into z as identification signals is performed.

[0042] Next, a flowchart for a program incorporated into the computer 13 or 14 in which the secret rule has been registered is shown in Figure 8. The flowchart will be briefly described based on Figure 8. In S7, it is determined whether or not the identification signal A and NZ have been received. The program waits until they are received. When they are received, the program advances to S8, where it is determined whether or not the difference between the current time and NZ is within a tolerance K seconds. When the difference is not within the tolerance K seconds, the program advances to S12, where the process of outputting a determination that the access to the equipment is not permissible is performed, and the program returns to S7. The tolerance K is a delay time period obtained in consideration of the time period required to calculate the identification signal in the wrist watch 33 or the time period required for data communication to the computer 13 or 14 in which secret rule has been registered. The tolerance K is a short period of time of, for example, 3 seconds or the like.

[0043] When the difference is within the tolerance K by S8, the program advances to S9, where it is determined whether or not the tolerance K seconds or more has passed since the preceding receiving time up to the current identification signal receiving time. When the tolerance K seconds or more has not passed, the program advances to S12, where it is determined that the access is not permissible. It is included in the conditions for permitting an access that the tolerance K seconds or more has passed since the preceding receiving time up to the current identification signal receiving time in order to prevent an inconvenience that, for the period of the tolerance K seconds after the identification signal A and NZ are transmitted, a system abuser records and transmits the identification signal A and NZ to the computer

13 or 14 in which the secret rule has been registered so as to illegally access the equipment.

[0044] When it is determined that the tolerance K seconds have passed by S9, the program advances to S10, where the process of substituting the input signal consisting of the current time into w, x, y, of the secret function f(w, x, y, z) registered beforehand, substituting the NZ into z to calculate the answer B is performed. The program advances to S11, where it is determined whether or not the B is equal to the received A. If they are not equal, the program advances to S12, where it is determined that the access is not permissible. If they are equal, the program advances to S13, where the process of outputting a determination that the access to the equipment is permissible is performed. Then, the program returns to S7.

[0045] Next, another embodiment of this individual identification system will be described.

(1) As an input signal into the secret function, a numeral, which is common nationwide or worldwide and which increases or decreases over-time based on the code/data broadcasting is used instead of the current time. In this case, the numeral for the input signal may be transmitted from a identification signal input terminal such as the register 19, the CAPTAIN terminal 18 or the like. The transmission means to the device 33 owned by the equipment user may be either through radio wave or cable.

[0046] Furthermore, the device 33 owned by the equipment user is not limited to a wrist watch and may be any individual terminal such as a handheld electronic calculator or the like.

[0047] (2) As means for selecting an unused signal to be used as the input signal, a function for rejecting an input signal which has been used in the past is added to computer 13 or 14 in which the secret rule has been registered. A flowchart of a program to be incorporated into the computer 13 or 14 in which the secret rule has been registered and a flowchart of a program to be incorporated into the device 33 owned by the equipment user in such a case are respectively shown in Figure 9(A) and (B).

[0048] The flowcharts shown in Figure 9(A) and (B) will be briefly described. First, the program incorporated into the device 33 owned by the equipment user will be described based on Figure 9(B). In S22, the initial value of I is set to "1". Then, the program advances to S23, where it is determined whether the transmission button 21 (see Figure 6) has been turned ON or not. The program waits until the transmission button 21 is turned ON. When the transmission button 21 is turned ON, the program advances to S24, where the process of substituting the I into the secret function f(x) and calculating the value A of f(I) is performed. At this stage, the I is "1". Next, the program advances to S25, where the process of outputting the respective values of A and I as identification signals is performed. The program advances to S26, where the process of adding "1" to the current value of I to make a new value of I is performed. Thereafter, the program returns to S23.

[0049] Thus, in the case where the first access is attempted using the device 33 owned by the equipment user, the identification signal A calculated by substituting I=1 into the f(I) is transferred to the computer 13 or 14 in which the secret rule has been registered. In the case where the second access is attempted, I=2 when the transmission button 21 of the device 33 owned by the equipment user is turned ON to calculate the identification signal A. Therefore, the iden-

tification signal A calculated by substituting I=2 into f(I) is transferred.

[0050] Thus, in the device 33, each time the transmission button 21 is turned ON to perform an access operation, I is updated as a result of addition of "1". Therefore, each time an access operation is performed, a different value of I is used. As a result, a different identification signal A is calculated and transferred each time.

[0051] Next, the program incorporated into the computer 13 or 14 in which the secret rule has been registered will be described based on Figure 9(A). By S14, the initial value of J is set to "1". The program advances to S15, where it is determined whether the identification signals A and I transferred from the device 33 have been received or not, and the program waits until they are received. When they are received, the program advances to S16, where it is determined whether J=I or not. During the first access operation, J is "1" and I should be "1". Therefore, it should be determined to be YES by S16. However, a person who attempts to illegally access the equipment cannot decide the current value of I. Accordingly, it is considered that he/she substitutes an arbitrary value to I and transfers the value to the computer 13 or 14. In such a case, it is determined to be NO by S16. The program advances to S17, where the process of outputting a determination that the access to the equipment is not permissible is performed, and the program returns to S15.

[0052] When it is determined that J=I, the program advances to S18, where the process of substituting J into the registered secret function f(x) to calculate the answer B is performed. Then, the program advances to S19, where it is determined whether the calculated B and the transferred A are equal to each other or not. When they are not equal, the

program advances to S17, where it is determined that the access to the equipment is not permissible. When they are equal, the program advances to S20, where the process of outputting a determination that the access to the equipment is permissible is performed. Then, the program advances to S21, where the process of updating J by adding "1" to the current value of J is performed, and then the program returns to S15.

[0053] Thus, the computer 13 or 14 in which the secret rule has been registered updates the value of J by adding "1" each time the identification signals A and I are transferred from the device 33. As a result, the current value of I in the device 33 and the current value of J in the computer 13 or 14 in which the secret rule has been registered should be in synchronization with each other and identical.

[0054] (3) It is structured that a secret rule of a person who is the subject of the manipulation such as a fugitive or the like is registered and when an identification signal is transferred to a computer in which the secret rule has been registered, a signal instructing to notify the location is returned to the terminal to which the identification signal was input, and a signal indicating the location where the terminal is installed is transferred from the terminal to a computer of the police.

[0055] (4) As the secret rule used for the individual identification, a secret rule used for the above-described invention of digital signature is used. In other words, a secret rule owned by a person is used both for the digital signature system and the individual identification system.

[0056] Next, the various embodiment described above will be listed below.

(1) In the individual identification system (access control system), a function of rejecting an input signal which has been used in the past is provided to the determination means as the means for selecting an unused signal to be used.

[0057] (2) In the individual identification system, a numeral which is common nationwide and increases or decreases whenever selected to be used or over-time is used as the input signal as the means for selecting an unused signal to be used.

[0058] (3) In the individual identification system described in (2) above, the numeral is defined based on the signal transferred by the code/data broadcasting.

[0059] (4) In the individual identification system described in (2) or (3) above, the numeral represents the current year, month, day and time.

[0060] (5) In the individual identification system described in (2) above, the device of the equipment user is constituted of a wrist watch, and the time displayed by the wrist watch is used as the input signal.

[0061] (6) In the individual identification system described in (5) above, the wrist watch can display time based on the signal transferred by the code/data broadcasting.

[0062] (7) In the individual identification system described in (3) or (6) above, the code/data broadcasting is transmitted from individual piece of equipment which are the targets of utilization.

[0063] (8) In the individual identification system described in (5) or (6) above, the wrist watch has a signal transmission section to the human hand so as to transfer the output

identification signal to the equipment which is the target of utilization via the human hand as the medium.

[0064] (9) In the individual identification system, the device owned by the equipment user is structured to stop the function for individual identification when a prescribed signal from the signal transmitter owned by the owner of the device cannot be received.

[0065] Next, the correspondence between the elements of present invention and the above-described embodiments will be described. Secret conversion data specific to an access demander is constituted by the secret function f(w, x, y, z) or f(I), f(x) shown in Figure 9. A personal calculation device storing the secret conversion data specific to an access demander is constituted by the device 33 owned by the equipment user. As described above, variable data which is used both in the personal calculation device and for the access permission or denial determination means (described below) and which is variable between the preceding access time and the present access time is constituted by the current time shown in S5 of Figure 7 and S10 of Figure 8, or I shown in S24 of Figure 9 and J shown in S18. As described above, the personal calculation device has an operation function for converting the above-selected variable data by a prescribed algorithm in accordance with the secret conversion data.

[0066] The access permission or denial determination means for determining whether an access is permitted or not is constituted by the computer 13 or 14 in which the secret rule has been registered. As described above, the converted data obtained by the conversion by the personal calculation device (identification signal such as A or the like) is transferred to the access permission or denial determination means by the data communication (see Figure 4). The access

permission or denial determination means determines whether the transferred converted data is appropriate or not based on the above-selected conversion data.

[0067] The access target to which the access demander attempts to access is constituted by the bank 10, the data bank 11 or the coin locker 12. The authentication means which is installed at a different location from that of the access target, can perform data communication with the access target side, and performs centralized management by performing comprehensive authentication for access control is constituted by the computer 13 or 14. As described above, when the access demanding side transfers the password data to the access target side, the password data is forwarded to the authentication means by data communication.

[0068] The data for determination for determining whether the password data is appropriate or not is constituted by the secret function f(w, x, y, z) in S10 of Figure 8. The authentication means stores data for determination, of the access demanding side, for determining whether the password data is appropriate or not. Using the data for determination, the authentication means determines whether the forwarded password data is appropriate or not and thus performs authentication (S11 in Figure 8). The authentication means returns the result to the access target side from which the password data has been forwarded.

[0069] As described above, the access target side permits the access of the access demander on the conditions that the result indicating that the password data is appropriate is returned.

[0070] The commonly changing data which is commonly changeable in the access demanding side and the authentication means side and is changeable access by access is constituted

by the input signal consisting of the current time in S5 of Figure 7 or I in S24 of Figure 9(B). The variable password data, the content of which is variable access by access using the commonly changing data is constituted by the answer A in S5 of Figure 7 or A in S25 of Figure 9(B). The variable password data generation means for generating, on the access demanding side, the variable password data, the content of which is variable access by access using the commonly changing data is constituted by the wrist watch 33. The data receiving means for receiving variable password data generated by the variable password data generation means and transferred by data communication is constituted by S7 of Figure 8. The time synchronous authentication means for performing authentication by determining whether the variable password data received by receiving means is appropriate or not by using, as the commonly changing data, the time variable data which changes in accordance with time is constituted by S8 through S11 of Figure 8. The prescribed tolerable error authentication means which, even when the variable password data received by the data receiving means is generated by the time variable data having an error, does not prohibit an access based on the error when the error is within a prescribed tolerable time period (tolerable value K seconds) is constituted by S8 of Figure 8. The unauthorized access prohibition means for, when an access is made by variable password data which is identical with the variable password data used for preceding access within the tolerable time period from the preceding access, determining that such an access is not permitted is constituted of S9 of Figure 8. The automatic error correction means for, when an error occurs in the time variable data by a malfunction of the clock of the variable password data generation means, automatically correcting the error so that over-time accumulation of the errors can be prevented is constituted by S1 and S2 of Figure 7.

[0071] The identification signal input acknowledgement means for acknowledging that an identification data signal for identifying a person possessing the variable password data generation means is input is constituted by S3 of Figure 7 described above. On the conditions that the input is acknowledged to be performed by the identification signal input acknowledgement means, the generation of the variable password data becomes possible (on the conditions that it is determined Yes by S3 of Figure 7, the processing in S4 through 6 becomes possible). As described above, the authentication means executes a password authentication operation on the conditions that a result confirming that the password is appropriate based on the registration confirmation data (calling number) notified by the access demander for confirming whether or not the access demander has been registered beforehand (the result confirming that the calling number is a usable number belonging to a person registered beforehand) is obtained before the authentication means performs the password authentication operation based on the variable password data.

[Effect of the Invention] According to the first invention, data for authentication is registered in the authentication means for performing centralized management by performing comprehensive authentication for access control. By this, when an access demander transmits variable password data in an attempt to access either one of a plurality of access targets, the variable password data is forwarded to the authentication means and authentication is performed by the authentication means. Accordingly, even if there are a number of access targets, it is not necessary to register the data for authentication in each of the many access targets. Thus, various inconveniences which occur when the data for authentication is registered in each of the many access targets can be prevented to a maximum degree. Furthermore, the forwarded password data is determined to be appropriate or

not for authentication using, as the commonly changing data, the time variable data which changes in accordance with time. Accordingly, the content of the variable password data is different between the preceding access and the present access, thus improving the security. In the case when an error occurs in the time variable data by a clock of a malfunction of the variable password data generation means, the error is automatically corrected so that over-time accumulation of the errors can be prevented. Accordingly, the inconveniences such that access becomes impossible by the error in the time variable data or the like can be prevented to a maximum degree. According the second invention, data for authentication is registered in the authentication means for performing centralized management by performing comprehensive authentication for access control. By this, when an access demander transmits variable password data in an attempt to access either one of a plurality of access targets, the variable password data is forwarded to the authentication means and authentication is performed by the authentication means. Accordingly, even if there are a number of access targets, it is not necessary to register the data for authentication in each of the many access targets. Thus, various inconveniences which occur when the data for authentication is registered in each of the many access targets can be prevented to a maximum degree. Furthermore, the forwarded password data is determined to be appropriate or not for authentication using, as the commonly changing data, the time variable data which changes in accordance with time. Accordingly, the content of the variable password data is different between the preceding access and the present access, thus improving the security. Moreover, even when the forwarded variable password data is generated by the time variable data having an error, an access is not prohibited based on the error when the error is within a prescribed tolerable time period. Accordingly, inconveniences such as an access being impossible because of a slight error or the

like can be prevented to a maximum degree. In the case where a prescribed tolerable time period is provided, it is conceivable that an illegal conduct is performed of eavesdropping the variable password data during input or transfer and using the same variable password data to perform an illegal access within the prescribed tolerable time period. In other words, since an access with an error is not prohibited during the tolerable time period, there is a risk that the variable password having the same content is accepted a plurality of times and thus the tolerable time period becomes a loophole in security. According to the present invention, when an access is made with the variable password which is the same as the password as used in the preceding access within the tolerable time period from the preceding access, such an access is not determined to be permissible, so that an illegal access during the tolerable time period can be prevented. This further improves the security.

[Brief Description of the Drawings]
[Figure 1] A perspective view.
[Figure 2] A flowchart.
[Figure 3] A function illustrating view.
[Figure 4] A function illustrating view.
[Figure 5] A function illustrating view.
[Figure 6] A perspective view.
[Figure 7] A flowchart.
[Figure 8] A flowchart.
[Figure 9] (A) and (B) are each a flowchart.
[Figure 10] A control circuit configuration of a personal terminal device.

[Description of the Reference Numerals]
3 is a personal terminal device; 2 is an input device; 1 is a keyboard; 33 is a wrist watch; 13 and 14 are computers; 10 is a bank; 11 is a data bank; 12 is a coin locker; 25 is a transmitter.

Japanese Patent No. 2884338

[Abstract]

[Problem] Even if there are a number of access targets, to eliminate the necessity of registering data for determination for determining whether the password data is appropriate or not in each pieces of the access target equipment, to minimize the risk of misappropriation of the registered data for determination.

[Means for Solving the Problem] A secret function f(w, x, y, z) which is the data for determination for determining whether or not the password data sent from an access demander is appropriate is registered in the computer 13 or 14. To whichever one of a plurality of pieces of access target equipment 10, 11 or 12 the access is demanded, the password transferred to the access target equipment is forwarded to the computer 13 or 14, and authentication is performed by determining whether the password data is appropriate or not comprehensively by the computer 13 or 14. The result is returned to the access target equipment from which the password data has been forwarded.

Japanese Patent No. 2884338

Fig.1

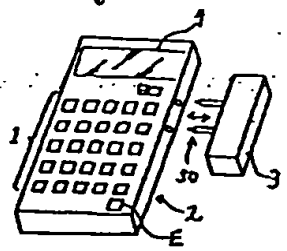


Fig.4

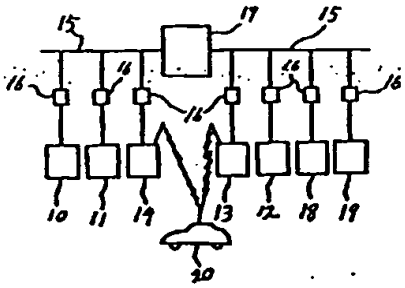


Fig.5

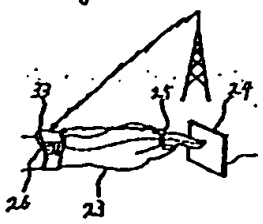


Fig.6

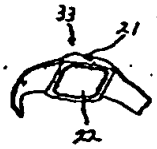


Fig.2

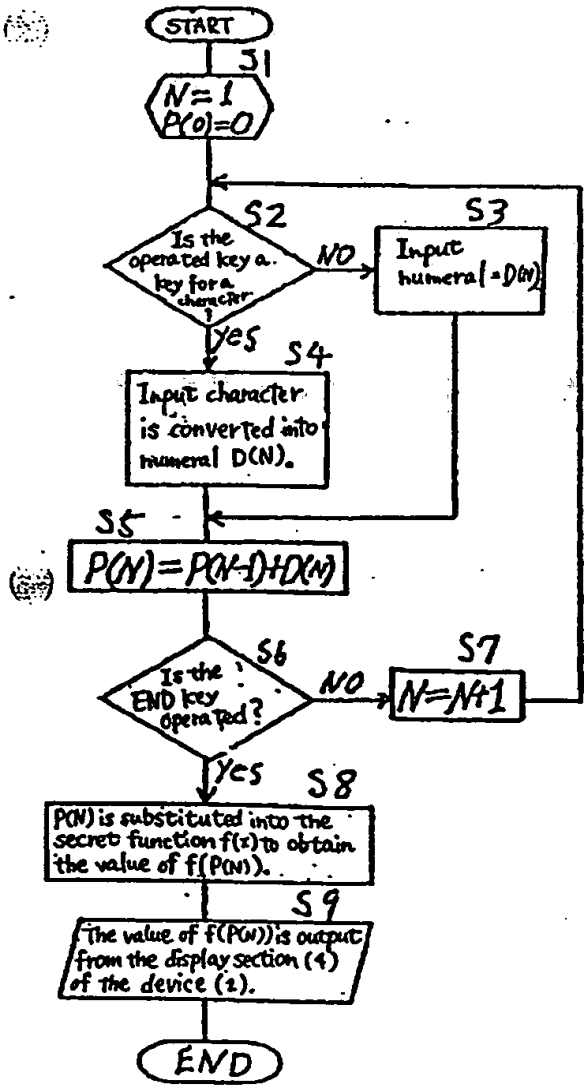


Fig.3

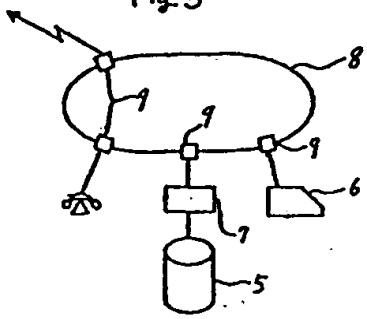
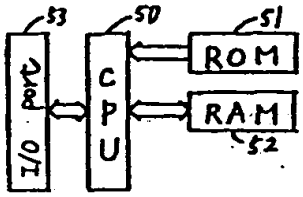
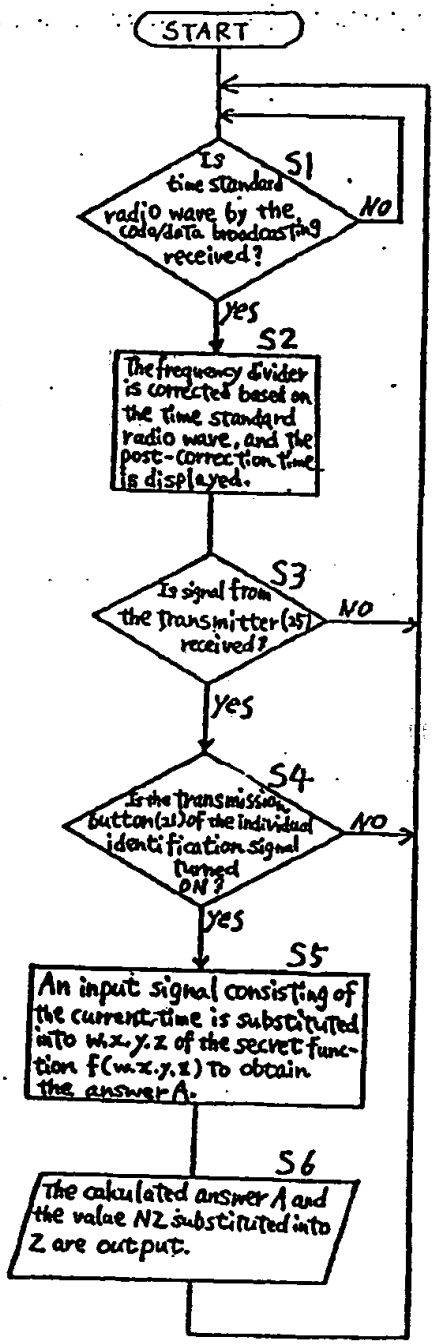


Fig.10



Japanese Patent No. 2884338

Fig. 7



SHUSAKU YAMAMOTO

Re: Japanese Patents 2835433 and 2884338 of Fujiwara

Patent No. 2884338

<Indication>
Indication No. 1
Items registered
Filing date: October 11, 1984
Application number: 09-264850
Date of allowance: December 17, 1998
Number of inventions: 2
Title of the Invention: Access control system
Registration date: February 12, 1999

<Records on issue fee>
Issue fee
Year 1: 21,800 yen, paid on January 12, 1999
Year 2: 21,800 yen, paid on January 12, 1999
Year 3: 21,800 yen, paid on January 12, 1999

<Ownership>
Items registered
1st owner:
Yutaka TSUKAMOTO
40-15, Oaza Kitano, Oyodo-cho, Yoshino-gun,
Nara-ken
Registration date: February 12, 1999

2nd owner:
[Transfer of the right]
Acceptance date: April 8, 1999
Acceptance number: 001200
822-2, Tsuchigahara, Tamano-shi, Okayama-ken
Kaneko FUJIWARA
Registration date: April 28, 1999

SHUSAKU YAMAMOTO

Re: Japanese Patents 2835433 and 2884338 of Fujiwara

3rd owner:

[Partial transfer of the right]

Acceptance date: August 30, 1999

Acceptance number: 003184

35-2, 5-chome, Utsukushigaoka, Aoba-ku,

Yokohama-shi, Kanagawa-ken

Kabushiki Kaisha Laurel Intelligent Systems

Registration date: September 24, 1999

October 29, 1999